mN

Notice of Allowability	Application No.	Applicant(s)	
	10/713,303	SYMES, DOMINIC HUGO	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *10/31/2007*.

2. ☒ The allowed claim(s) is/are *1,3-15 and 17-29*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *10/26/2007* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

Examiner's Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

In view of ***Pre-appeal request*** filed on 10/18/2007 and an authorization for this Examiner's Amendment given in a telephone interview with John R. Lastova (Reg. No. 33,149) on 26 October 2007, the claimed subject matters are further distinctly pointed out as patentable features to place the application in the condition for allowance.

This application has been amended as follows:

IN THE CLAIMS

Cancel claims 2, 16 and 30.

Replace claims 1, 3, 4, 12, 13, 15, 17, 18, 26, 27, and 29 as follows.

Claim 1:

A data processing apparatus, comprising:

a processor configured in a plurality of modes and a plurality of domains, said plurality of domains comprising a secure domain and a non-secure domain, said plurality of modes including at least one non-secure mode being a mode in the non-secure domain, at least one secure mode being a mode in the secure domain, and a monitor mode, said processor being configured such that when executing a program in a secure mode said program has access to secure data which is not accessible when said processor is operating in a non-secure mode;

a storage unit configured to store processor configuration data comprising data controlling access to memory by the processor;

said processor being configured at least partially in said monitor mode to execute a monitor program to manage switching between said secure domain and said non-secure domain, said switching including switching the processor configuration data in the storage unit between secure processor configuration data and non-secure processor configuration data;

when in said monitor mode, said monitor program being configured to use monitor mode specific processor configuration data, thereby ensuring that operation of the processor in said monitor mode is unaffected by the switching of the processor configuration data so that the ability of the monitor program to perform the switching of processor configuration data is not compromised.

Claim 3:

A data processing apparatus as claimed in Claim ~~2~~ 1, wherein the memory is configured to store data required by the processor and comprises secure memory for storing the secure data and non-secure memory for storing non-secure data, said processor configuration data comprising memory permission data identifying whether the processor is allowed to access said secure data.

Claim 4:

A data processing apparatus as claimed in Claim ~~2~~ 1, wherein said processor configuration data comprises memory space configuration data identifying which areas of memory are accessible by the processor.

Claim 12:

A data processing apparatus as claimed in Claim ~~2~~ 1, further comprising:

a memory management unit configured, upon receipt of a memory access request from the processor, to perform one or more predetermined access control functions to control issuance of the memory access request to the memory;

said monitor mode specific processor configuration data indicating that said memory management unit is disabled in said monitor mode.

Claim 13:

A data processing apparatus as claimed in Claim ~~2~~ 1, wherein said memory includes a cache, and said monitor mode specific processor configuration data indicates that the processor is not allowed to use said cache to access data in said monitor mode.

Claim 15:

A method of managing processor configuration data in a data processing apparatus comprising a processor configured in a plurality of modes and a plurality of domains, said plurality of domains comprising a secure domain and a non-secure domain, said plurality of modes including at least one non-secure mode being a mode in the non-secure domain, at least one secure mode being a mode in the secure domain, and a monitor mode, said processor being configured such that when executing a program in a secure mode said program has access to secure data which is not accessible when said processor is operating in a non-secure mode, said method comprising the steps of:

executing on said processor at least partially in said monitor mode a monitor program to manage switching between said secure domain and said non-secure domain, including performing the step of switching the processor configuration data comprising data controlling access to memory by the processor between secure processor configuration data and non-secure processor configuration data;

when in said monitor mode, said monitor program using monitor mode specific processor configuration data, thereby ensuring that operation of the processor in said monitor mode is unaffected by the switching of the processor configuration data so that the ability of the monitor program to perform the switching of processor configuration data is not compromised.

Claim 17:

A method as claimed in Claim ~~16~~ 15, wherein the memory is configured to store data required by the processor and comprises secure memory for storing the secure data and non-secure memory for storing non-secure data; said processor configuration data comprising memory permission data identifying whether the processor is allowed to access said secure data.

Claim 18:

A method as claimed in Claim ~~16~~ 15, wherein said processor configuration data comprises memory space configuration data identifying which areas of memory are accessible by the processor.

Claim 26:

A method as claimed in Claim ~~16~~ 15, further comprising the step of:

upon receipt of a memory access request from the processor, employing a memory management unit to perform one or more predetermined access control functions to control issuance of the memory access request to the memory;

said monitor mode specific processor configuration data indicating that said memory management unit is disabled in said monitor mode.

Claim 27:

A method as claimed in Claim ~~16~~ 15, wherein said memory includes a cache, and said monitor mode specific processor configuration data indicates that the processor is not allowed to use said cache to access data in said monitor mode.

Claim 29:

A computer program encoded in a computer-readable medium executable to configure a processor in a data processing apparatus to manage processor configuration data, the processor, when executing the computer program, being configured in a plurality of modes and a plurality of domains, said plurality of domains comprising a secure domain and a non-secure domain, said plurality of modes including at least one non-secure mode being a mode in the non-secure domain, at least one secure mode being a mode in the secure domain, and a monitor mode, said processor being configured such that when executing a program in a secure mode said program has access to secure data which is not accessible when said processor is operating in a non-secure mode, the processor, when executing said computer program being configured to perform the steps of:

while at least partially in said monitor mode, managing switching between said secure domain and said non-secure domain, including performing the step of switching the processor configuration data comprising data controlling access to memory by the processor between secure processor configuration data and non-secure processor configuration data; and

when in said monitor mode, using monitor mode specific processor configuration data, thereby ensuring that operation of the processor in said monitor mode is unaffected by the switching of the processor configuration data so that the ability of the monitor program to perform the switching of processor configuration data is not compromised.

Allowable Subject Matter

Claims 1, 3 – 15 and 17 – 29 are allowed.

The following is an examiner's statement of reasons for allowance:

The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations recited in claims 1, 15 and 29 (& associated dependent claims).

The prior arts on record fail to teach or suggest a processor configured in a plurality of modes and a plurality of domains, said plurality of domains comprising a secure domain and a non-secure domain, said plurality of modes including at least one non-secure mode being a mode in the non-secure domain, at least one secure mode being a mode in the secure domain, and a monitor mode; a storage unit configured to store processor configuration data comprising data controlling access to memory by the processor; said processor being configured at least partially in said monitor mode to execute a monitor program to manage switching between said secure domain and said non-secure domain, said switching including switching the processor configuration data in the storage unit between secure processor configuration data and non-secure processor configuration data; when in said monitor mode, said monitor program being configured to use monitor mode specific processor configuration data, thereby ensuring that operation of the processor in said monitor mode is unaffected by the switching of

the processor configuration data so that the ability of the monitoring program to perform the switching of processor configuration data is not compromised.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100